REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-8 are pending in the present application. Claims 1 and 4-8 are amended by the present amendment. Claim amendments and find support in the application as originally filed.[1] Thus, no new matter is added.

In the outstanding Office Action, Claims 1-8 are rejected under 35 U.S.C. § 103(a) as unpatentable over Bayer et al. (U.S. Pat. No. 6,311,190, herein "Bayer") in view of Kalpio et al. (U.S. Pat. No. 6,343,323, herein "Kalpio" in view of Shrader et al. (U.S. Pat. No. 6,374,359, herein "Shrader") in view of Byrne (U.S. Pat. No. 6,223,288). Applicants respectfully traverse the rejections.

Claim 4 is directed to an information providing method that includes, in part, recording, receiving, selecting, generating and transmitting steps. A third receiving step includes receiving, at a key server, user terminal identification from a user terminal used by a user. A verifying step includes verifying the registration of the user terminal by comparing the user terminal identification received by the third receiving step with the user terminal identification stored by the second recording step. A generating step includes generating a key to manage downloaded content from the content server based on a result of the verifying step. A second transmission step includes transmitting, from the key server, the key and the target destination of said contents server which enables the user terminal used by said user to download contents from said contents server. Independent Claims 1 and 5-8 include similar features.

In a non-limiting example, Applicants' Fig. 1 shows an information providing system having a registration apparatus 3 that receives from the user terminal 1 a) a request for

[1] Amendments find support at least in Figure 29.

transmission of the user registration form data and b) user terminal identification data specifying said user terminal as an argument of a target destination of the registration server said attributes input by said user. The registration apparatus 3 selects the registration form data based on the attributes received by said first receiving step. The user registration form data, as illustrated in Figs. 8 and 9, is transmitted and recorded in the user terminal 1. The registration server 3 receives a user profile based on what is input on the form and records the profile data and the terminal identification data in the user terminal 1. The registration apparatus 3 then sends a program to the user terminal 1 for accessing a key server 5. The key server 5 receives the user terminal identification and compares the received terminal identification with the terminal indemnification data recorded earlier in the user terminal 1. Using the result of this comparison, if the user terminal requesting a key is registered the key server generates a key based on the user terminal identification. Once this is accomplished, the target destination of the contents server (4-1 through 4-4), in the form of a URL, back to the user terminal 1 allowing the user to download content. Additionally, the key server sends a key based on the user terminal identification data specifying of the user terminal used by the user, allowing the user to manage the downloaded content. Claims 6-8 include similar features but directed to a user terminal.

Turning now to the rejection of Claims 1-8 in the outstanding Office Action, Applicants respectfully traverses the §103(a) rejection of Claims 1-8 based on Bayer, Kalpio, Shrader and Byrne for the following reasons.

Amended Claim 1 recites, in part,

> second recording means for recording said user profile data in association with said user terminal identification specifying said user terminal used by said user;
>
> second transmitting means for transmitting a program for access to a key server; and
>
> a key server and content server, the key server comprising

> third receiving means for receiving the user terminal identification from the user terminal,
>
> verifying means for verifying registration of the user terminal by comparing the user terminal identification received by the third receiving means with the user terminal identification stored by the second recording means;
>
> generating means for generating a key to manage downloaded content from the content server based on a result of the verifying means,

Independent Claims 4-8 recite similar features.

Bayer describes a system in which a registration server provides a questionnaire form in an appropriate language to the user.

Kalpio describes a proxy server receiving a user ID from a client and transmitting the HTTP data to the client. Further, in Kalpio the client receives content from a WWW server via a proxy server.

In item 9 on page 4, the outstanding Office Action states that "Bayer and Kalpio did not teach generating a key based on user terminal identification." However, the outstanding Action relies on Shrader as teaching describing the generation of a key by a key server.

Shrader describes client-server web-based transaction which tests a web browser to ensure that a valid cookie has been set on the web-browser. Further, Shrader makes this determination by including the cookie (which includes the client IP address for which the cookie was issued) in an ASCII string which is sent to the server by a web-browser. The server then decrypts the ASCII string and compares the embedded IP address with the IP address of the web-browser that sent the ASCII string. In other words, the server is using the embedded IP address to determine if the web-browser which has the cookie installed is the same web-browser for which the cookie was issued.

In contrast, Claim 1 recites verifying registration of the user terminal by comparing the user terminal identification received by the third receiving means with the user terminal

identification stored by the second recording means and generating a key to manage downloaded content from the content server based on a result of the verifying.

In other words, Claim 1 recites checking if a user terminal is registered with the system and only generating a key for the user terminal if it is determined by comparing a user terminal identification sent by a user terminal with a user terminal identification stored on the server side that the user terminal is previously registered. In contrast, Shrader teaches sending a cookie to a user terminal. When the user terminal attempts to access the server, the server checks to see if the cookie is correctly installed by comparing the IP address of the sending user terminal with an IP address embedded in an encrypted portion of the same request. Therefore, ***in Shrader, the user terminal identification (IP address) is compared against data sent from the user terminal itself (ASCII embedded IP address)***, while ***in Claim 1 the user terminal identification sent by the user is compared with user terminal identification stored on the server side***.

Thus, the system recited in Claim 1 provides the advantage that even if a user terminal's hard-disk is wiped clean as a result of a crash, the user will not have to re-register the user terminal with the server. In contrast, in Shrader if the cookie stored in the web-browser is cleared the web-browser will have to be re-authenticated with the server.

Further, Shrader does not describe or suggest generating a key to manage downloaded content from the content server based on a result of the verifying. In the outstanding Action col. 2, lines 53-64, col. 4, lines 36-41 and col. 7, lines 50-65 of Shrader are cited in item 9 as describing generating a key to manage downloaded content from the content server. However, these portions of Shrader describe encrypting and decrypting a cookie to verify if a cookie has been installed on a user terminal. ***Nowhere in these portions or any other portion of Shrader is it taught or suggested that a key to manage downloaded content from the content server is generated based on a result of verifying the registration of the user***

terminal by comparing the user terminal identification received by the third receiving means with the user terminal identification stored by the second recording means.

Therefore, the features recited in amended Claim 1 patentably distinguish over the Bayer, Kalpio and Shrader references cited in the outstanding Action.

Further, Byrne describes a data encryption system which uses an executable program to download a key, however, Byrne does not cure the above noted deficiencies in Bayer, Kalpio and Shrader with regard to Claim 1.

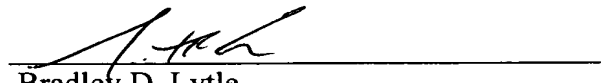
Therefore, Applicants respectfully submit that Claim 1 and consequently independent Claims 4-8 patentably distinguish over Bayer, Kalpio, Shrader and Byrne considered alone or together in any proper combination.

Accordingly, Applicants submit that independent Claims 1 and 4-8, and claims depending therefrom, are allowable.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Scott A. McKeown
Registration No. 42,866

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\JL\211391US\211391US_AM(12.13.2006).DOC